Incident Response Policy

Stratum Intelligence Inc. · Version 1.4 · Effective June 2026

1. Purpose

This policy defines how Stratum detects, responds to, and communicates security incidents affecting the platform or Customer data. It applies to all employees, contractors, and sub-processors.

2. Severity classification

- SEV-1 — confirmed unauthorised access to Customer data, cross-tenant data exposure, or full platform outage.
- SEV-2 — partial outage, degraded ingestion, or a security finding with credible exploit path.
- SEV-3 — limited-scope bug, single-tenant degradation, or a security finding without an exploit path.
- SEV-4 — informational issues and near-misses.

3. Roles

- Incident Commander — drives the response and owns the timeline.
- Communications Lead — owns customer and regulator communications.
- Scribe — captures the timeline and decisions in the incident channel.
- Subject Matter Experts — pulled in as required.

4. Response timeline

- Detection to acknowledgement: 15 minutes for SEV-1/2.
- Customer notification: within 48 hours of confirming a Personal Data Breach affecting their tenant.
- Regulator notification: within 72 hours where required by law, coordinated with affected Customers.
- Post-incident review: published internally within 5 business days; customer-facing summary within 10 business days for SEV-1 and SEV-2.

5. Communications

SEV-1 and SEV-2 incidents are posted to status.stratum.example in real time. Direct notifications go to the Customer's designated security contacts via email.

Stratum will never ask Customers to disclose credentials during an incident. All requests for evidence flow through the incident commander and are logged.

6. Evidence and forensics

Immutable audit logs, ingest traces, and connector heartbeats are retained for at least 365 days. Forensic snapshots are taken before any remediation that would alter affected systems.

7. Post-incident review

Every SEV-1 and SEV-2 produces a blameless post-mortem covering root cause, contributing factors, timeline, and corrective actions with named owners and due dates.

8. Contact

Report a suspected incident to security@stratum.example or via the vulnerability disclosure form at /legal/vdp. PGP key available on request.